

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2002年5月10日 (10.05.2002)

PCT

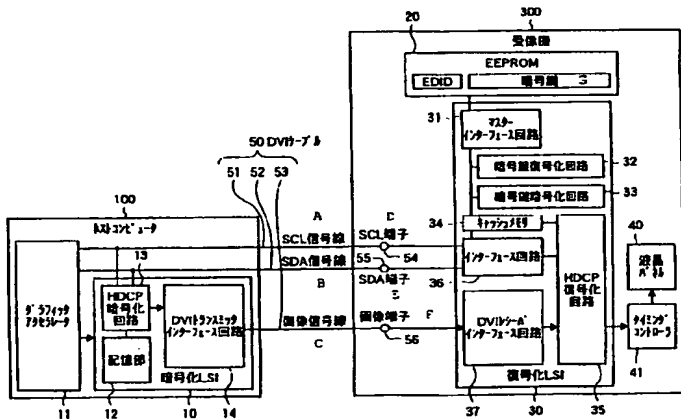
(10) 国際公開番号
WO 02/37285 A1

- (51) ●国際特許分類: G06F 12/14, G09G 5/00, H04N 7/16, 1/00, 1/44
- (21) 国際出願番号: PCT/JP01/09279
- (22) 国際出願日: 2001年10月23日 (23.10.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2000-331533 2000年10月30日 (30.10.2000) JP
特願2001-112042 2001年4月10日 (10.04.2001) JP
- (71) 出願人 (米国を除く全ての指定国について): ザインエレクトロニクス株式会社 (THINE ELECTRONICS, INC.) [JP/JP]; 〒104-0032 東京都中央区八丁堀1丁目10番7号 マツダ八重洲通ビル6階 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 挟間克樹 (HAZAMA, Katsuki) [JP/JP]. 桑山克己 (KUWAYAMA, Katsumi) [JP/JP]; 〒104-0032 東京都中央区八丁堀1丁目10番7号 マツダ八重洲通ビル6階 ザインエレクトロニクス株式会社内 Tokyo (JP).
- (81) 指定国 (国内): CA, CN, IL, IN, JP, KR, RU, SG, US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[続葉有]

(54) Title: SEMICONDUCTOR INTEGRATED CIRCUIT, RECEIVER APPARATUS USING THE SAME, RECEIVER APPARATUS MANUFACTURING METHOD AND REPAIRING METHOD, AND VIDEO PROVIDING METHOD

(54) 発明の名称: 半導体集積回路、それを用いた受信側装置、受信側装置の製造方法及び修理方法、並びに、画像提供方法



100...HOST COMPUTER
10...ENCRYPTING LSI
11...GRAPHIC ACCELERATOR
13...HDCP ENCRYPTING CIRCUIT
12...STORING UNIT
14...DVI TRANSMITTER INTERFACE CIRCUIT
50...DVI CABLES
A...SCL SIGNAL LINE
B...SDA SIGNAL LINE
C...VIDEO SIGNAL LINE
D...SCL TERMINAL
E...SDA TERMINAL
F...VIDEO TERMINAL
300...RECEIVER

G...ENCRYPTION KEY
30...DECRYPTING LSI
31...MASTER INTERFACE CIRCUIT
32...ENCRYPTION KEY DECRYPTING CIRCUIT
33...ENCRYPTION KEY ENCRYPTING CIRCUIT
34...CACHE MEMORY
36...INTERFACE CIRCUIT
37...DVI RECEIVER INTERFACE CIRCUIT
35...HDCP DECRYPTING CIRCUIT
40...LIQUID CRYSTAL PANEL
41...TIMING CONTROLLER

(57) Abstract: In a receiver or the like for reproducing encrypted video signals, a semiconductor integrated circuit wherein the number of the components used therein has been reduced and wherein, after completion of the receiver hardware, information can be written into a nonvolatile memory and the written information can be rewritten. This semiconductor integrated circuit is one for use in an apparatus for receiving encrypted video signals and has an interface circuit for effecting a serial communication with the exterior and also has a memory control circuit for controlling the nonvolatile memory to write and/or read a first information

[続葉有]



添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

to be transmitted to the exterior by the interface circuit and a second information to be used to decrypt the encrypted video signals.

(57) 要約:

暗号化された画像信号を再生する受像機等において、使用する部品点数を減らすことができ、且つ、受像機のハードウェア完成後に、不揮発性メモリに情報を書き込んだり、書き込まれた情報を書き換えることができる半導体集積回路。この半導体集積回路は、暗号化された画像信号を受信する装置において用いるための半導体集積回路であって、外部とシリアル通信を行うインターフェース回路と、インターフェース回路によって外部に送信される第1の情報、及び、暗号化された画像信号を復号化するために用いられる第2の情報を書き込み、及び／又は、読み出すように不揮発性メモリを制御するメモリ制御回路とを具備する。

明 細 書

半導体集積回路、それを用いた受信側装置、
受信側装置の製造方法及び修理方法、並びに、画像提供方法

5

技術分野

本発明は、一般的に半導体集積回路に関し、特に、暗号化された画像
信号を受信又は送信するために用いる半導体集積回路に関する。また、
本発明は、受信用の半導体集積回路を用いた受像機等の受信側の装置、
10 受信側の装置の製造方法及び修理方法に関する。さらに、本発明は、そ
のような受像機を用いた画像提供方法に関する。

背景技術

パーソナルコンピュータ等の送信側の装置とモニタやプロジェクタ等
15 の受信側の装置との接続に関するDDC (display data channel) と呼
ばれる規格は、受信側の装置が、送信側の装置から、その受信側の装置
にとって最適の信号を得られるように定められている。

DDC規格に従う受像機は、EDID (extended display identific
ation data) と呼ばれる情報が記憶されたEEPROM (electrically
20 erasable programmable read-only memory) を有している。EDID
には、受像機の種類、表示できる解像度、クロック周波数、メーカー名
、シリアル番号等の情報が含まれている。また、EDIDを記憶するE
EPROMとしては、2線式シリアルEEPROMが一般的に用いられ
、I²Cバス方式に準ずるシリアル通信によってデータが送受信される
25 (I²Cバスは、フィリップス社の登録商標)。

このシリアル通信においては、SDA (シリアルデータ) 端子及びS

CL（シリアルクロック）端子と呼ばれる2つの端子を用いて、受像機に内蔵されているEEPROMの制御と情報の送受信が行われる。受像機のSDA端子及びSCL端子がケーブルを介してパーソナルコンピュータに接続されると、パーソナルコンピュータは、EEPROMに記憶

5 されているEDIDを読み取ることができる。これにより、受像機にとって最適な信号に関する情報が、パーソナルコンピュータに提供される。

一方、パーソナルコンピュータ等から受像機に送信される画像信号は、アナログ信号からデジタル信号に移行しつつあり、画像信号の劣化が

10 ほとんど起こらないようになってきた。このため、画像信号の不法なコピー等から著作物を保護する必要が生じている。そのための手段の1つとして、パーソナルコンピュータ等から受像機に送信される画像信号を暗号化することが行われている。その中でも、現在、HDCP（high-bandwidth digital content protection）と呼ばれる方式が標準になり

15 つつある。

図1は、HDCP方式による従来の受像機を用いた画像伝送システムを示すブロック図である。図1に示すように、この画像伝送システムは、ホストコンピュータ100と受像機200とによって構成される。受像機200は、HDCP方式による暗号鍵情報（以下、「暗号鍵」とも

20 いう）を保有する。暗号鍵は、受像機200からDDCによってホストコンピュータ100に通知される「公開鍵」と、不特定多数に知られてはならない「秘密鍵」とを含んでいる。

ホストコンピュータ100は、高速で描画するための画像信号を生成するグラフィックアクセラレータ11と、HDCP方式による暗号化LSI10とを含んでいる。暗号化LSI10は、暗号鍵を記憶する記憶部12と、記憶部12に記憶されている暗号鍵を用いて画像信号を暗号

化するHDCP暗号化回路13と、画像信号の送信を行うDVIトランスミッタインターフェース回路14とを有している。HDCP方式においては、一般的に、画像信号の送受信にDVI (digital visual interface) 規格が用いられているので、画像信号を送信する回路及び受信する回路は、DVI規格に準拠している。

一方、受像機200は、EDIDを記憶するシリアルEEPROM221と、暗号鍵を記憶するEEPROM222と、HDCP方式によって暗号化された画像信号を暗号鍵を用いて復号化する半導体集積回路（復号化LSI）230と、液晶パネル240と、タイミングコントローラ241とを含んでいる。

復号化LSI230は、EEPROM222を制御するマスターインターフェース回路231と、HDCP復号化回路235と、暗号鍵等の送受信を行うインターフェース回路236と、画像信号の受信を行うDVIレシーバインターフェース回路237とを有している。

液晶パネル240は、復号化された画像信号に基づいて画像を表示する。また、タイミングコントローラ241は、液晶パネルの信号線に画像信号を入力するタイミングをコントロールする。

さらに、受像機200は、EEPROM221及びインターフェース回路236に接続されたSCL端子54及びSDA端子55と、DVIレシーバインターフェース回路237に接続された画像端子56とを有しており、これらの端子に接続されたDVIケーブル50を通じて外部の機器と信号の送受信を行う。DVIケーブル50は、DDC規格によるデータの送受信に用いられるSCL信号線51、SDA信号線52及び画像信号線53を含んでいる。

システムが起動されると、ホストコンピュータ100は、受像機200のEEPROM221に記憶されているEDIDと、EEPROM2

22に記憶されている公開鍵とを読み出すことができる。ホストコンピュータ100において、グラフィックアクセラレータ11は、受信されたEDIDに基づいて、受像機200に適した画像信号を生成する。また、受信された公開鍵に基づいて受像機200が認証された場合に、HDCP暗号化回路13は、暗号鍵を用いて画像信号を暗号化し、DVIトランスミッタインターフェース回路14は、これを受像機200に送信する。

受像機200において、マスターインターフェース回路231は、EEPROM222から暗号鍵を読み出して、HDCP復号化回路235に供給する。HDCP復号化回路235は、この暗号鍵を用いて、DVIレシーバインターフェース回路237によって受信された画像信号を復号化する。復号化された画像信号は、タイミングコントローラ241の制御の下で、液晶パネル240に表示される。

このような画像伝送システムにおいて、受像機200のEEPROM222に記憶されている公開鍵と秘密鍵とを含む暗号鍵の内、秘密鍵は不特定多数に知られてはならない。従って、パーソナルコンピュータ等によって自由に読み出すことができるEDIDと、読み出しに制限を加えなくてはならない暗号鍵とを、同じEEPROMに保存することはできなかった。そのため、従来は、DDC用の信号線に接続されたシリアルEEPROM221にEDIDのみを記憶させて、暗号鍵を記憶するためのEEPROM222を別に用意していた。画像信号を復号化する復号化LSI230は、EEPROM222を制御して暗号鍵を読み出し、パーソナルコンピュータ等からの要求に応じて公開鍵のみをDDC用の信号線に提供していた。

ところで、暗号鍵を保存するEEPROM222は、DDC用の端子であるSCL端子54及びSDA端子55には接続されていないものの

、汎用のEEPROMであるため、ROMリーダー／ライター等を用いることにより簡単にその内容を読み出すことができる。従って、暗号鍵が平文のままEEPROM222に記憶されると、一般にその内容を明らかにされる恐れがあった。そこで、暗号鍵が読み出されることを防ぐため、EEPROM222と復号化LSI230との間をモールド樹脂等で封印する方法が提案されている。

しかしながら、このような方法を採用したとしても、依然としてEDIDを記憶するEEPROMと暗号鍵を記憶するEEPROMとの2個のEEPROMが必要であり、部品点数の増加に伴うコストの上昇は避けられない。また、EDIDと暗号鍵という2種類の情報を別個にそれぞれのEEPROMに記憶させなくてはならないため、受像機の製造過程において、情報を記憶させる工程及びテスト工程が複雑となり、コストがかかっていた。さらに、EEPROMに暗号鍵を平文のまま書き込み、それを読み出すことができないように樹脂等で封印すると、故障等によりEEPROMを再度書き換える必要が生じて、EEPROMを書き換えることが不可能になってしまうという欠点があった。

発明の開示

そこで、上記の点に鑑み、本発明の第1の目的は、暗号化された画像信号を受信する受像機等の受信側の装置において使用する部品点数を減らすことができ、且つ、ハードウェアの完成後に不揮発性メモリに情報を再度書き込むことを可能とする半導体集積回路を提供することである。また、本発明の第2の目的は、受信側の装置に画像信号を送信する送信側の装置においてセキュリティを向上させることができる半導体集積回路を提供することである。さらに、本発明の第3の目的は、上記のような受信用の半導体集積回路を用いた受信側の装置を提供することであ

る。加えて、本発明の第4の目的は、受像機を用いた画像提供方法を実現することである。

以上の課題を解決するため、本発明の第1の観点に係る半導体集積回路は、暗号化された画像信号を受信する装置において用いるための半導体集積回路であって、外部とシリアル通信を行うインターフェース回路と、インターフェース回路によって外部に送信される第1の情報、及び、暗号化された画像信号を復号化するために用いられる第2の情報を書き込み、及び／又は、読み出すように不揮発性メモリを制御するメモリ制御回路とを具備する。

10 また、本発明の第2の観点に係る半導体集積回路は、暗号化された画像信号を受信する装置において用いるための半導体集積回路であって、不揮発性メモリに記憶されている暗号化された暗号鍵を復号化する暗号鍵復号化回路と、暗号鍵復号化回路によって復号化された暗号鍵を用いて画像信号を復号化する画像信号復号化回路とを具備する。

15 さらに、本発明の第3の観点に係る半導体集積回路は、画像信号を暗号化して受信側の装置に送信する装置において用いるための半導体集積回路であって、画像信号に所定の信号処理を施す画像処理回路と、所定の信号処理が施されていない画像信号と所定の信号処理が施された画像信号との内の一方を選択する選択回路と、選択回路によって選択された
20 画像信号を暗号化する暗号化回路と、受信側の装置から受信した暗号鍵に基づいて受信側の装置を認証するか否かについて判断し、受信側の装置が認証された場合には、所定の信号処理が施されていない画像信号を暗号化して出力するように選択回路及び暗号化回路を制御し、受信側の装置が認証されなかった場合には、所定の信号処理が施された画像信号
25 を暗号化しないで出力するように選択回路及び暗号化回路を制御する制御回路とを具備する。

本発明の 1 つの観点に係る受信側の装置は、暗号化された画像信号を受信する装置であって、外部とシリアル通信を行う第 1 の手段と、暗号化された画像信号を受信する第 2 の手段と、第 1 の手段によって外部に送信される第 1 の情報、及び、第 2 の手段によって受信された画像信号を復号化するために用いられる第 2 の情報を記憶するための不揮発性メモリと、不揮発性メモリに記憶されている第 2 の情報を用いて、第 2 の手段によって受信された画像信号を復号化する第 3 の手段とを具備する。

本発明の 1 つの観点に係る製造方法は、外部とシリアル通信を行う第 1 の手段と、暗号化された画像信号を受信する第 2 の手段と、不揮発性メモリとを有し、暗号化された画像信号を受信する装置を製造する方法であって、第 1 の手段を用いてシリアル通信を行うことにより、装置に関する第 1 の情報、及び、第 2 の手段によって受信された画像信号を復号化するために用いられる第 2 の情報を装置に入力するステップ (a) と、ステップ (a) において入力された第 1 及び第 2 の情報を不揮発性メモリに書き込むステップ (b) とを具備する。

本発明の 1 つの観点に係る画像提供方法は、暗号鍵を入力する第 1 の手段と、暗号化された画像信号を受信する第 2 の手段とを有し、暗号化された画像信号を受信して画像を表示する受像機を用いて画像を提供する方法であって、第 1 の手段によって受像機に入力された暗号鍵に基づいて、第 1 の手段によって受像機に入力された暗号鍵に基づいて、受像機を認証するか否かについて判断するステップ (a) と、ステップ (a) において受像機が認証された場合に、第 2 の手段によって受信された画像信号を第 1 の手段によって受像機に入力された暗号鍵を用いて復号化し、復号化された画像信号に基づいて画像を表示するステップ (b) とを具備する。

本発明によれば、受信用の半導体集積回路において、E D I Dと暗号鍵とを1つの不揮発性メモリに記憶させるので、受像機等の受信側の装置に用いられる部品点数を削減することができると共に、受信側の装置の製造過程における情報の書き込み工程及びテスト工程を簡略化することができる。また、ハードウェアの完成後に不揮発性メモリに情報を書き込んだり、書き換えることができるので、受信側の装置の製造が容易であり、出荷後に故障が起きても受信側の装置を修理することができる。さらに、暗号鍵を入力する第1の手段を有する受像機を用いることにより、暗号鍵を有する特定のユーザのみに画像を提供する画像提供方法を実現することができる。

また、本発明によれば、送信用の半導体集積回路において、受信側の装置を認証するか否かを判断し、認証しない場合には画質を劣化させる等の処理を行うので、外部のソフトウェアの助けを必要とせず、セキュリティを向上させることができる。

図面の簡単な説明

本発明の利点及び特徴は、以下の詳細な説明と図面とを関連させて考察すれば明らかになる。これらの図面において、同じ参照番号は同じ構成要素を指している。

図1は、従来の受像機を用いた画像伝送システムを示すブロック図である。

図2は、本発明の第1の実施形態に係る受信側の装置を用いた画像伝送システムを示すブロック図である。

図3は、本発明の第1の実施形態に係る受信側の装置の変形例を用いた画像伝送システムを示すブロック図である。

図4は、本発明の第1の実施形態に係る受信側の装置において不揮発

性メモリにE D I Dを書き込む動作を示すフローチャートである。

図5は、本発明の第1の実施形態に係る受信側の装置において不揮発性メモリに暗号鍵を書き込む動作を示すフローチャートである。

図6は、本発明の第1の実施形態に係る受信側の装置を用いて画像を
5 提供する方法を示すフローチャートである。

図7は、本発明の第2の実施形態に係る受信側の装置を用いた画像伝送システムを示すブロック図である。

図8は、本発明の第2の実施形態に係る受信側の装置を用いて画像を提供する方法を示すフローチャートである。

10 図9は、本発明の第1の実施形態に係る送信側の装置を用いた画像伝送システムを示すブロック図である。

図10は、本発明の第2の実施形態に係る送信側の装置を用いた画像伝送システムを示すブロック図である。

15 発明を実施するための最良の形態

図2は、本発明の第1の実施形態に係る受信側の装置を用いた画像伝送システムを示すブロック図である。以下の実施形態においては、受信側の装置として、液晶パネル等の表示装置を有する受像機を用いる場合について説明するが、表示装置を受信側の装置に含めない構成として、

20 受信側の装置に外部の表示装置を接続するようにしても良い。

図2に示すように、この画像伝送システムは、ホストコンピュータ100と受像機300とによって構成される。受像機300は、HDCP方式による暗号鍵を保有する。暗号鍵は、受像機300からDDCによってパーソナルコンピュータ100に通知される公開鍵と、不特定多数
25 に知られてはならない秘密鍵とを含んでいる。

ホストコンピュータ100は、高速で描画するための画像信号を生成

するグラフィックアクセラレータ 11 と、暗号化 L S I 10 とを含んでいる。暗号化 L S I 10 は、暗号鍵を記憶する記憶部 12 と、記憶部 12 に記憶されている暗号鍵を用いて画像信号を暗号化する H D C P 暗号化回路 13 と、D V I 規格に従って画像信号の送信を行う D V I トランスミッタインターフェース回路 14 とを有している。

ホストコンピュータ 100 には、S C L 信号線 51 と、S D A 信号線 52 と、画像信号線 53 とを含む D V I ケーブル 50 を介して、受像機 300 が接続されている。

受像機 300 は、E D I D 及び暗号鍵を記憶する不揮発性メモリとして E E P R O M 20 と、H D C P 方式によって暗号化された画像信号を暗号鍵を用いて復号化する半導体集積回路（復号化 L S I）30 と、復号化された画像信号に基づいて画像を表示するデバイスとして液晶パネル 40 と、液晶パネルの信号線に画像信号を入力するタイミングをコントロールするタイミングコントローラ 41 とを含んでいる。なお、不揮発性メモリとしては、シリアル E E P R O M、パラレル E E P R O M、フラッシュ E E P R O M の他に、一般的な P R O M や電池内蔵の S R A M 等を用いることができる。また、画像を表示するデバイスとしては、液晶パネル 40 の他に、P D P (plasma display panel) や C R T (cathode ray tube) を用いても良い。

20 復号化 L S I 30 は、E E P R O M 20 を制御するマスターインターフェース回路 31 と、暗号鍵復号化回路 32 と、暗号鍵暗号化回路 33 と、キャッシュメモリ 34 と、暗号鍵等の送受信を行うインターフェース回路 36 と、画像信号の復号化を行う H D C P 復号化回路 35 と、画像信号の受信を行う D V I レシーバインターフェース回路 37 とを内蔵している。なお、復号化 L S I 30 が E E P R O M 20 等の不揮発性メモリを内蔵するようにしても良い。あるいは、H D C P 復号化回路 35

及びDVIレシーバインターフェース回路37と、それ以外の回路とを、別個の半導体集積回路に形成しても良い。

インターフェース回路36は、EDIDや暗号鍵等の情報の送受信を制御する。また、インターフェース回路36は、I²Cバス方式による
5 通信において、スレーブデバイスとして動作する。インターフェース回路36は、SCL端子54及びSDA端子55に接続されており、SCL信号線51及びSDA信号線52を介して外部との信号の送受信を行う。

キャッシュメモリ34は、EEPROM20に書き込まれる情報を一時的に保存したり、EEPROM20から読み出された情報を一時的に保存する。キャッシュメモリ34としては、SRAM (static random
10 access memory) を用いることができる。

暗号鍵暗号化回路33は、平文で入力された暗号鍵を暗号化する。暗号化された暗号鍵は、マスターインターフェース回路31によってEEPROM20に保存される。なお、暗号化された暗号鍵が復号化LSI
15 30に入力される場合には、暗号鍵暗号化回路33は不要である。

暗号鍵復号化回路32は、暗号化された暗号鍵を平文に復号化する。復号化された暗号鍵は、暗号化された画像信号を復号化する際に用いられる。

20 マスターインターフェース回路31は、EEPROM20との間における信号の送受信を制御し、EEPROM20に対して情報の書き込みや読み出しを行う。また、マスターインターフェース回路31は、EEPROM20に書き込むべき情報と、EEPROM20に書き込まれた情報とを比較(ベリファイ)し、EEPROM20に書き込まれた内容
25 の信頼性を高める動作モードを有している。この動作モードは、復号化LSI30のテストモードにおいて設定することができる。

EEPROM20に暗号化された暗号鍵が記憶されている場合には、暗号鍵復号化回路32が、暗号化された暗号鍵を平文に復号化し、マスターインターフェース回路31が、復号化された暗号鍵を入力された鍵と比較する。マスターインターフェース回路31は、EEPROM20
5 に情報が正しく書き込まれたか否かをチェックするために、エラー検出コード又はエラー訂正コードを計算してEEPROM20に書き込まれた情報を検証するようにしても良い。

あるいは、図3に示すように、受像機400において、フラッシュEEPROM62を内蔵したマイクロコンピュータ61を用いるようにし
10 ても良い。マイクロコンピュータ61は、インターフェース回路36又はキャッシュメモリ34との間で信号の送受信を行い、内蔵するEEPROM62に対して情報の書き込みや読み出しを行う。その場合には、復号化LSI60がマスターインターフェース回路を内蔵する必要はない。

15 再び図1を参照すると、HDCP復号化回路35は、HDCP方式による暗号鍵を用いて、DVIレシーバインターフェース回路37によって受信された画像信号を復号化する。

DVIレシーバインターフェース回路37は、画像端子56に接続されており、画像信号線53を介してデジタル画像信号を受信する。D
20 VIレシーバインターフェース回路37は、DVI規格に準拠しており、RGB（赤、緑、青）の3つの画像信号チャンネルについて、エンコードされて送信されるシリアルデータをパラレルデータに変換する。

I²Cバス方式による通信においては、それぞれのスレーブデバイスにスレーブアドレスが割り振られている。例えば、一般的に、EDID
25 の送受信には、読み出し用としてアドレス「A0h」、書き込み用としてアドレス「A1h」が割り振られている。また、HDCP方式による

レシーバには、読み出し用としてアドレス「76h」、書き込み用としてアドレス「77h」が割り振られている。本実施形態におけるインターフェース回路36は、HDCP方式によるレシーバに割り当てられているスレーブアドレス「7Ah」及び「7Bh」と同様に、EDIDの
5 応答に割り当てられているスレーブアドレス「A0h」及び「A1h」を指定されたときにも応答するように設計されている。

一方、受像機のホスト側に用いられるHDCP方式によるトランスミッタには、HDCP方式による暗号鍵等の送受信用としてアドレス「78h」及び「79h」、トランスミッタの物理層の設定用にアドレス「
10 70h」及び「71h」が割り振られている。

次に、本実施形態に係る受信側の装置においてDDC規格によるEDIDを書き込む動作について、図2及び図4を参照しながら説明する。EDIDを記憶するEEPROM20においては、その誤動作を防ぐために、画像制御信号の1つであるVSYNC信号（vertical synchroni
15 zing signal：垂直同期信号）を用いることが一般的である。本実施形態においても、EDIDの書き込み及び読出しの制御においては、VSYNC信号を併せて用いている。

図4は、本実施形態に係る受信側の装置において、不揮発性メモリにEDIDを書き込む動作を示すフローチャートである。この書き込み動作は、受信側の装置のハードウェアの完成後に行われる。
20

ステップS101において、ホストコンピュータ100等の外部機器がスレーブアドレスA1hを指定してEDIDを送信すると、受像機300の復号化LSI30は、SCL端子54及びSDA端子55を用いてEDIDを受信する。

25 ステップS102において、インターフェース回路36は、受信したEDIDをキャッシュメモリ34に一旦保存する。

ステップS103において、マスターインターフェース回路31は、キャッシュメモリ34に保存された内容をEEPROM20に書き込む。或いは、マスターインターフェース回路31は、EDIDをキャッシュメモリ34から読み出しながら、並行してEEPROM20にこれを
5 書き込んで良い。

次に、本実施形態に係る受信側の装置においてHDCP方式による暗号鍵を書き込む動作について、図2及び図5を参照しながら説明する。

図5は、本実施形態に係る受信側の装置において、不揮発性メモリにHDCP方式による暗号鍵を書き込む動作を示すフローチャートである
10 。この書き込み動作も、受信側の装置のハードウェアの完成後に行われる。

ステップS201において、ホストコンピュータ100等の外部機器がスレーブアドレス77hを指定して暗号鍵を送信すると、受像機300の復号化LSI30は、SCL端子54及びSDA端子55を用いて
15 暗号鍵を受信する。

ステップS202において、インターフェース回路36は、受信した暗号鍵をキャッシュメモリ34に一旦保存する。

ステップS203において、復号化LSI30は、キャッシュメモリ34に保存されている暗号鍵について、暗号化が必要であるか否かを判
20 断する。即ち、暗号鍵をEEPROM20に平文のままで保存すると、暗号鍵が一般に漏れてしまう恐れがある。そこで、受像機の製造者は、暗号鍵を信頼性高く保存したい場合には、暗号鍵を暗号化してEEPROM20に保存することができるようになっている。この暗号化のため
25 にも良いし、予め暗号化されている暗号鍵を復号化LSI30に送信しても良い。

復号化LSI30内で暗号鍵を暗号化する場合には、ステップS204において、暗号鍵暗号化回路33が暗号鍵を暗号化してからステップS205に移行する。このようにして、暗号鍵を暗号化するモードを設けることにより、受像機において暗号鍵を信頼性高く保存することができる。

ここで、暗号鍵の暗号化においては、画像信号の暗号化における暗号化強度と同等以上の暗号化強度が必要である。また、暗号鍵を暗号化するモードに移行する方法については、一般ユーザに理解されにくい方法が用いられ、これを公開しないことにより、暗号化のアルゴリズムを秘匿することができる。例えば、特殊なコマンドを復号化LSI30に入力したときに、暗号鍵暗号化回路33が活性化されて、暗号鍵を暗号化するモードに移行するようにしても良い。そのような特殊なコマンドにおいても、画像信号を暗号化する際の暗号化強度と同等以上のセキュリティ性が必要である。

一方、あらかじめ暗号化された暗号鍵を受信した場合や、セキュリティ性があまり高くないため平文のまま保存しても構わない暗号鍵を受信した場合には、ステップS205に直接移行する。ステップS205において、マスターインターフェース回路31が、暗号鍵をEEPROM20に書き込む。

なお、EDIDや暗号鍵をEEPROM20に書き込む際に用いるデータフォーマットは、復号化LSI30で読み出すことが可能なデータフォーマットであれば良く、DDC規格で定められたものと異なっている構わない。例えば、エラー検出コード又はエラー訂正コードを含むデータフォーマットを用いても良い。

本実施形態によれば、以上述べたEDIDや暗号鍵を保存するためのEEPROMを1つに集約することができる。また、HDCP方式によ

る暗号鍵を暗号化することにより、暗号鍵が保存されているEEPROM20と復号化LSI30との間をモールドで固める必要がなくなる。受像機の製造工程において、EDID及び暗号鍵の書き込みは、ハードウェアの完成後に、SCL端子54及びSDA端子55を用いて行うことができる。また、受像機の出荷後にEEPROM20の内容に不良が発見された場合に、修理作業としてEDID及び暗号鍵の書き込みを行うこともできる。

次に、本実施形態に係る受信側の装置を用いて画像を提供する方法について、図2及び図6を参照しながら説明する。図6は、本実施形態に係る受信側の装置を用いて画像を提供する方法を示すフローチャートである。

まず、ステップS301において、受像機300の電源を投入し、ステップS401において、ホストコンピュータ100の電源を投入する。

15 受像機300の電源が投入されると、受像機300は、ステップS302において、EEPROM20に書き込まれたEDID及び暗号鍵を読み出してキャッシュメモリ34に保存し、ホストコンピュータ100からの要求に対応する準備を整える。この準備動作は、電源投入時に限らず、マイクロコンピュータ等の制御により行っても良い。

20 ホストコンピュータ100は、ステップS402において、SCL端子54及びSDA端子55を通じてEDIDのアドレスA0h及びA1hを指定して、EDIDの送信を要求する。これに応答して、受像機300は、ステップS303において、キャッシュメモリ34に保存されている情報を利用し、インターフェース回路36を介して、あたかも復
25 号化LSI30がEDID専用のEEPROMであるかのような振る舞いをして、EDIDをホストコンピュータ100に送信する。ホストコ

ンピュータ100は、ステップS403において、EDIDを受信して受像機300に関する情報を解読する。

なお、受像機300の復号化LSI30は、電源が投入されていなくても、ホストコンピュータ100からEDIDの送信を要求されたら、
5 DVIケーブルを介してホストコンピュータ100から供給される電源によって動作して、EDIDを送信しなければならない。一般的に、ホストコンピュータは5Vの電源電圧を供給するが、復号化LSIの動作電圧は3.3Vであり、受像機において降圧回路が必要になる。また、利用できる電流は50mAが目安であり、復号化LSIをフルに動作さ
10 せるとこの電流値をオーバーしてしまう。従って、受像機に電源が投入されていないときにEDIDを送信するためには、消費電流についての配慮も必要である。

受像機300は、ステップS304において、暗号鍵が暗号化されているか否かを判断する。即ち、受像機300の復号化LSI30は、E
15 EPROM20から暗号鍵が読み出されると、暗号鍵が暗号化されているか否かを自動認識する。暗号鍵が暗号化されていると判断された場合には、ステップS305において、暗号鍵復号化回路32が暗号鍵を復号化し、ステップS306において、復号化された暗号鍵をキャッシュメモリ34に保存する。一方、暗号鍵が暗号化されていないと判断され
20 た場合には、ステップS306において、暗号鍵をそのままキャッシュメモリ34に保存する。

ホストコンピュータ100が、ステップS404において、SCL端子54及びSDA端子55を用いてHDCP方式による公開鍵等の情報を要求すると、受像機300は、ステップS307において、キャッシュメモリ34に保存されている情報を利用し、インターフェース回路3
25 6を介してホストコンピュータ100に公開鍵等の情報を送信する。こ

ここで、インターフェース回路 36 は、HDCP 方式による秘密鍵を平文のままホストコンピュータ 100 に送信することではなく、HDCP 方式による秘密鍵が一般に公開されるリスクを低減している。

ホストコンピュータ 100 は、ステップ S 405 において、受像機 300 から公開鍵を受信すると、ステップ S 406 において、公開鍵に基づいて受像機 300 を認証するか否かについて判断する。具体的には、ホストコンピュータ 100 が、受信した公開鍵とホスト側の公開鍵とに基づいて、乱数と秘密鍵とを用いた演算を行い、演算結果が一致した場合に、受像機 300 を認証する。

10 ホストコンピュータ 100 は、受像機 300 が認証された場合に、ステップ S 407 において、画像信号の暗号化を行い、ステップ S 408 において、暗号化された画像信号を受像機 300 に送信する。

受像機 300 は、ステップ S 308 において、暗号化された画像信号を受信する。即ち、DVI レシーバインターフェース回路 37 が、画像
15 信号線 53 を介してシリアルデータとして送信される RGB 各チャンネルのデジタル画像信号を受信し、パラレルデータに変換する。次に、ステップ S 309 において、復号化 LSI 30 の HDCP 復号化回路 35 が、キャッシュメモリ 34 に保存されている HDCP 方式による暗号鍵を用いて、暗号化されたパラレルデータを復号化する。

20 ステップ S 310 において、復号化されたデジタル画像信号は、タイミングコントローラ 41 を介して液晶パネル 40 に出力され、画像が表示される。

本実施形態においては、画像信号を伝送する際に用いられる情報として、画像信号を暗号化したり復号化したりするために用いられる暗号鍵
25 を例にとって説明した。しかしながら、画像信号を送受信する際に用いられる情報は、暗号鍵に限らず、例えば、送受信される画像信号を表示

するために受像機を最適な状態に設定する情報であっても良い。そのような情報としては、画像の出力タイミングの設定情報、PLL (phase locked loop) の設定情報、画像サイズや色の補正に用いられる情報等が挙げられる。

- 5 次に、本発明の第2の実施形態に係る受信側の装置について説明する。本実施形態に係る受信側の装置は、外部から暗号鍵等の情報を入力する手段をさらに具備するものである。

図7は、本発明の第2の実施形態に係る受信側の装置を用いた画像伝送システムを示すブロック図である。ここでは、外部から暗号鍵等の情報を入力する手段として、受像機500にICカードを読み書きするカードリーダー/ライター21を設けている。復号化LSI70のマスタ
10 ーインターフェース回路38は、所定の暗号鍵が記録されたICカードが受像機300に挿入されると、EEPROM20に優先してカードリーダー/ライター21によって読み出された暗号鍵をキャッシュメモリ
15 34に記憶させる。その他の構成については、本発明の第1の実施形態に係る受信側の装置と同様である。

なお、外部から暗号鍵等の情報を入力する手段としては、カードリーダー/ライター21の替わりに、赤外線リモコンによって送信された信号から情報を読み取る赤外線検出ユニットを設けても良い。その場合に
20 は、視聴者が、受像機のリモートコントローラ等进行操作することにより、暗号鍵等の情報を受像機に入力することができる。

次に、本実施形態に係る受信側の装置を用いて画像を提供する方法について、図7及び図8を参照しながら説明する。この画像提供方法によれば、ホストコンピュータと同様の機能を有するセットトップボックス
25 等に接続された複数のモニタ（受像機）の中で、特定の暗号鍵が供給されたモニタのみが画像を出力することを可能にする。

図 8 は、本実施形態に係る受信側の装置を用いて画像を提供する方法を示すフローチャートである。

まず、視聴者は、ステップ S 5 0 1 において、画像情報等のコンテンツの提供者に対して、所望のコンテンツの料金を支払うか、料金を支払
5 うことを約束する。これに応じて、提供者は、ステップ S 6 0 1 において、公開鍵が書き込まれた I C カードを視聴者に配付する。また、提供者は、ステップ S 6 0 2 において、このような視聴者のためにコンテンツを送信する。

視聴者が、ステップ S 5 0 2 において、I C カードをモニタに挿入す
10 ると、ステップ S 5 0 3 において、セットトップボックスは、I C カードに書き込まれた公開鍵を読み取って、公開鍵に基づいて、このモニタを認証するか否かの判断を行う。モニタが認証されると、ステップ S 5 0 4 において、送信されているコンテンツがモニタに受信され、モニタの画面に表示される。ここで、ステップ S 5 0 3 及びステップ S 5 0 4
15 における動作の詳細については、図 6 のステップ S 3 0 2 ~ S 3 1 0 及びステップ S 4 0 2 ~ 4 0 8 に示す動作と同様である。この画像提供方法によれば、コンテンツのために料金を支払った視聴者のみが、そのコンテンツの提供を受けることができる。

なお、この画像提供方法においては、公開鍵を入力する媒体として I
20 C カードを用いたが、視聴者が、受像機のリモートコントローラに備えられたテンキーを用いて公開鍵をモニタに送信しても良いし、ゲーム機のコントローラと O S D (open software description) とを用いて公開鍵をモニタに入力しても良い。その他、コンテンツの提供者又は視聴者が、電話回線を用いて公開鍵を配布しても良い。

25 次に、本発明の第 1 の実施形態に係る送信側の装置について説明する。これまで、H D C P 技術は、パーソナルコンピュータにおいて使用さ

れることが前提となっていた。パーソナルコンピュータが画像信号を暗号化して送信するためには、パーソナルコンピュータのDVIトランスミッタインターフェース回路と、モニタのDVIレシーバインターフェース回路との間で公開鍵の通信を行って、モニタを認証するか否かの判断を行わなくてはならない。その後、パーソナルコンピュータは画像信号の暗号化を開始し、モニタは画像信号の復号化を開始する。この一連の制御動作は、HDCP方式のダウストリームと呼ばれている。

ここで、パーソナルコンピュータは、ワードプロセッサや表計算のソフトウェアが稼動している場合には画像信号を暗号化する必要がなく、DVDディスクを再生する場合等に限って画像信号を暗号化する必要が生じる。また、モニタがHDCP方式に対応していない場合には、DVDディスクを再生できない等の表示を行うか、画質を低下させて再生するといった処理を行わなくてはならない。このような制御動作は、オペレーションソフトとグラフィックアクセラレータに内蔵されているHDCP制御回路との連携で行われ、HDCP方式のアップストリームと呼ばれている。

このように、従来の送信側の装置においては、送信側の暗号化LSIと受信側の復号化LSIだけでは画像信号の伝送制御を行うことができず、外部のソフトウェアの助けを必要としたため、セキュリティに関して問題があった。本実施形態に係る送信側の装置は、このような問題を解決したものである。

図9は、本発明の第1の実施形態に係る送信側の装置を用いた画像伝送システムを示すブロック図である。受信側の装置については、図2に示す受像機300と同一である。送信側の装置600は、DVDディスク等から画像信号を再生する画像信号再生回路601と、暗号鍵を記憶するための記憶部602と、記憶部602に記憶されている暗号鍵を用

いて、画像信号再生回路601によって再生された画像信号を暗号化して受像機300に送信する暗号化LSI80とを含んでいる。

暗号化LSI80は、画像信号に所定の信号処理を施す画像処理回路81と、画像信号再生回路601から出力される画像信号と画像処理回路81から出力される画像信号との内の一方を選択する選択回路82と、選択回路82によって選択された画像信号を暗号化する暗号化回路83と、暗号化回路83によって暗号化された画像信号を送信する物理層回路84と、暗号化制御回路85とを内蔵している。

暗号化制御回路85は、受信した暗号鍵に基づいて受信側の装置を認証するか否かについて判断し、受信側の装置が認証された場合には、所定の信号処理が施されていない画像信号を暗号化して出力するように選択回路82及び暗号化回路83を制御し、受信側の装置が認証されなかった場合には、所定の信号処理が施された画像信号を暗号化しないで出力するように選択回路82及び暗号化回路83を制御する。

次に、本実施形態に係る送信側の装置の動作について詳しく説明する。

送信側の装置600に電源が投入されると、暗号化制御回路85は、DVIケーブル50の電源線57を介して受像機300の一部の回路に電源を投入し、受像機300のEEPROMからEDIDを読み出す。

これにより、受像機300にとって最適な画像信号を知ることができる。EDIDを読み出せなかった場合や、EDIDを読み出してもHDCP方式に対応していない受像機であると判断した場合には、暗号化制御回路85は、保護を必要とするコンテンツを送信できないと判断する。

暗号化制御回路85は、受像機300がHDCP方式に対応していると判断すると、暗号化回路83と受像機300のHDCP復号化回路を制御して、HDCP方式による受像機の認証を開始する。具体的には、

暗号化制御回路 8 5 が、受信した公開鍵とホスト側の公開鍵とに基づいて、乱数と秘密鍵とを用いた演算を行い、演算結果が一致した場合に、受像機を認証する。

- 受像機が認証されると、暗号化制御回路 8 5 は、画像再生回路 6 0 1
- 5 から出力される画像信号を選択するように選択回路 8 2 を制御し、暗号化回路 8 3 に画像信号の暗号化を開始させる。なお、暗号化制御回路 8 5 は、ホットプラグ信号線 5 8 によって、受像機 3 0 0 に電源が投入されているか否かを検知して、受像機 3 0 0 に電源が投入されるまで画像信号の送信を行わないようにしても良い。
- 10 一方、受像機の認証が所定の時間内に完了しなかった場合には、暗号化制御回路 8 5 は、画像処理回路 8 1 を活性化させ、画像処理回路 8 1 から出力される画像信号を選択するように選択回路 8 2 を制御し、暗号化回路 8 3 に画像信号を平文のまま出力させる。画像処理回路 8 1 は、
- 15 入力される画像信号の解像度を低下させる処理を施したり、入力される画像信号にノイズを混入させる処理を施したり、入力される画像信号の代わりにコンテンツを送信できない旨のコメントを表す画像信号を出力したりする。これにより、受信側の装置が認証されなかった場合には、受像機 3 0 0 の画面において、保護する必要のない低品位の画像を表示したり、コンテンツを送信できない旨のコメントを表示したりすること
- 20 ができる。

次に、本発明の第 2 の実施形態に係る送信側の装置について説明する。本実施形態においては、選択回路を暗号化回路の後段に配置しており、この点が図 9 に示す装置と異なっている。

- 図 1 0 は、本発明の第 2 の実施形態に係る送信側の装置を用いた画像
- 25 伝送システムを示すブロック図である。受信側の装置については、図 2 に示す受像機 3 0 0 と同一である。

送信側の装置 700 に含まれている暗号化 LSI 90 は、画像再生回路 601 から出力された画像信号を暗号化する暗号化回路 91 と、画像再生回路 601 から出力された画像信号に所定の信号処理を施す画像処理回路 92 と、暗号化回路 91 から出力される画像信号と画像処理回路 92 から出力される画像信号との内の一方を選択する選択回路 93 と、選択回路 93 によって選択された画像信号を送信する物理層回路 94 と、暗号化制御回路 95 とを内蔵している。

暗号化制御回路 95 は、受信した暗号鍵に基づいて受像機 300 を認証するか否かについて判断し、受像機 300 が認証された場合には、所定の信号処理が施されていない画像信号を暗号化して出力するように選択回路 93 を制御し、受像機 300 が認証されなかった場合には、所定の信号処理が施された画像信号を暗号化しないで出力するように選択回路 93 を制御する。

次に、本実施形態に係る送信側の装置の動作について詳しく説明する。

暗号化制御回路 95 は、受像機 300 が HDCP 方式に対応していると判断すると、暗号化回路 91 と受像機 300 の HDCP 復号化回路を制御して、HDCP 方式による受像機の認証を開始する。受像機が認証されると、暗号化制御回路 95 は、暗号化回路 91 に画像再生回路 601 から出力される画像信号の暗号化を開始させ、暗号化回路 91 から出力される画像信号を選択するように選択回路 93 を制御する。

一方、受像機の認証が所定の時間内に完了しなかった場合には、暗号化制御回路 95 は、画像処理回路 92 を活性化させ、画像処理回路 92 から出力される画像信号を選択するように選択回路 93 を制御する。これにより、受信側の装置が認証されなかった場合には、受像機 300 の画面において、保護する必要のない低品位の画像を表示したり、コンテ

ンツを送信できない旨のコメントを表示したりすることができる。

以上、本発明を実施形態に基づいて説明したが、本発明は上記の実施形態に限定されることなく、特許請求の範囲に記載される範囲内で自由に変形及び変更することが可能である。

5

産業上の利用可能性

本発明は、画像信号を暗号化して送信するコンピュータ等の送信側の装置、及び、暗号化された画像信号を受信して復号化するモニタやプロジェクタ等の受信側の装置において利用することが可能である。さらに

10 、本発明は、そのような受像機を用いて画像を提供するビジネスにおいて利用することが可能である。

請 求 の 範 囲

1. 暗号化された画像信号を受信する装置において用いるための半導体集積回路であって、
- 5 外部とシリアル通信を行うインターフェース回路と、
前記インターフェース回路によって外部に送信される第1の情報、及び、暗号化された画像信号を復号化するために用いられる第2の情報を書き込み、及び／又は、読み出すように不揮発性メモリを制御するメモリ制御回路と、
- 10 を具備する半導体集積回路。
 2. 前記第1の情報が、前記装置に関するE D I D (extended display identification data) を含む、請求項1記載の半導体集積回路。
 3. 前記第2の情報が、画像信号を復号化するために用いられる暗号鍵を含む、請求項1記載の半導体集積回路。
- 15 4. 前記不揮発性メモリに記憶されている暗号化された暗号鍵を復号化する暗号鍵復号化回路をさらに具備する請求項3記載の半導体集積回路。
 5. 外部から供給された暗号鍵を暗号化する暗号鍵暗号化回路をさらに具備する、請求項4記載の半導体集積回路。
- 20 6. 前記暗号鍵暗号化回路が、画像信号の暗号化強度と同等以上の暗号化強度で暗号鍵を暗号化する、請求項5記載の半導体集積回路。
 7. 前記暗号鍵暗号化回路が、前記半導体集積回路に所定のコマンドが入力されたときに活性化される、請求項5記載の半導体集積回路。
 8. 前記メモリ制御回路が、前記不揮発性メモリに情報が正しく書き込まれたか否かをチェックするために、エラー検出コード又はエラー訂正
- 25 コードを計算して前記不揮発性メモリに書き込まれた情報を検証する、

請求項 1 記載の半導体集積回路。

9. 前記不揮発性メモリをさらに具備する請求項 1 記載の半導体集積回路。

10. 前記不揮発性メモリに記憶されている内容を一時的に保存するメモリをさらに具備する請求項 1 記載の半導体集積回路。

11. 暗号化された画像信号を受信する受信回路と、

前記不揮発性メモリに記憶されている第 2 の情報を用いて、前記受信回路によって受信された画像信号を復号化する画像信号復号化回路と、をさらに具備する請求項 1 記載の半導体集積回路。

10. 12. 前記画像信号復号化回路が、HDCP (high bandwidth digital content protection) に準拠する方式で暗号化された画像信号を復号化する、請求項 11 記載の半導体集積回路。

13. 暗号化された画像信号を受信する装置において用いるための半導体集積回路であって、

15. 不揮発性メモリに記憶されている暗号化された暗号鍵を復号化する暗号鍵復号化回路と、

前記暗号鍵復号化回路によって復号化された暗号鍵を用いて画像信号を復号化する画像信号復号化回路と、を具備する半導体集積回路。

20. 14. 画像信号を暗号化して受信側の装置に送信する装置において用いるための半導体集積回路であって、

画像信号に所定の信号処理を施す画像処理回路と、

所定の信号処理が施されていない画像信号と所定の信号処理が施された画像信号との内の一方を選択する選択回路と、

25. 前記選択回路によって選択された画像信号を暗号化する暗号化回路と

受信側の装置から受信した暗号鍵に基づいて前記受信側の装置を認証するか否かについて判断し、前記受信側の装置が認証された場合には、所定の信号処理が施されていない画像信号を暗号化して出力するように前記選択回路及び前記暗号化回路を制御し、前記受信側の装置が認証されなかつた場合には、所定の信号処理が施された画像信号を暗号化しないで出力するように前記選択回路及び前記暗号化回路を制御する制御回路と、

を具備する半導体集積回路。

15 1 5. 画像信号を暗号化して受信側の装置に送信する装置において用いるための半導体集積回路であって、

画像信号を暗号化する暗号化回路と、

画像信号に所定の信号処理を施す画像処理回路と、

暗号化された画像信号と所定の信号処理が施された画像信号との内の一方を選択する選択回路と、

15 受信側の装置から受信した暗号鍵に基づいて前記受信側の装置を認証するか否かについて判断し、前記受信側の装置が認証された場合には、所定の信号処理が施されていない画像信号を暗号化して出力するように前記選択回路を制御し、前記受信側の装置が認証されなかつた場合には、所定の信号処理が施された画像信号を暗号化しないで出力するように前記選択回路を制御する制御回路と、

20 を具備する半導体集積回路。

1 6. 暗号化された画像信号を受信する装置であって、

外部とシリアル通信を行う第1の手段と、

暗号化された画像信号を受信する第2の手段と、

25 前記第1の手段によって外部に送信される第1の情報、及び、前記第2の手段によって受信された画像信号を復号化するために用いられる第

2 の情報を記憶するための不揮発性メモリと、

前記不揮発性メモリに記憶されている第2の情報をを用いて、前記第2の手段によって受信された画像信号を復号化する第3の手段と、
を具備する装置。

- 5 17. 前記不揮発性メモリが、前記装置に関するEDID (extended display identification data) を第1の情報として記憶する、請求項16記載の装置。

18. 前記不揮発性メモリが、画像信号を復号化するために用いられる暗号鍵を第2の情報として記憶する、請求項16記載の装置。

- 10 19. 前記不揮発性メモリが、暗号化された暗号鍵を第2の情報として記憶し、

前記装置が、前記不揮発性メモリに記憶されている暗号化された暗号鍵を復号化する暗号鍵復号化手段をさらに具備する、請求項18記載の装置。

- 15 20. 外部から供給された暗号鍵を暗号化する暗号鍵暗号化手段をさらに具備する、請求項19記載の装置。

21. 前記不揮発性メモリが、シリアルEEPROM (electrically erasable programmable read-only memory) を含む、請求項16記載の装置。

- 20 22. 前記不揮発性メモリを制御するためのマイクロコンピュータをさらに具備する請求項16記載の装置。

23. 前記不揮発性メモリに記憶されている内容を一時的に保存するメモリをさらに具備する請求項16記載の装置。

24. 前記第3の手段が、HDCP (high bandwidth digital content
25 protection) に準拠する方式で暗号化された画像信号を復号化する、
請求項16記載の装置。

25. 暗号化された画像信号を受信する装置であって、
暗号鍵を入力する第1の手段と、
暗号化された画像信号を受信する第2の手段と、
前記第1の手段によって入力された暗号鍵を用いて、前記第2の手段
5 によって受信された画像信号を復号化する第3の手段と、
を具備する装置。
26. 前記第1の手段が、ICカードに記憶された情報を読み取る、請求項25記載の装置。
27. 前記第1の手段が、赤外線リモコンによって送信された信号から
10 情報を読み取る、請求項25記載の装置。
28. 外部とシリアル通信を行う第1の手段と、暗号化された画像信号を受信する第2の手段と、不揮発性メモリとを有し、暗号化された画像信号を受信する装置を製造する方法であって、
前記第1の手段を用いてシリアル通信を行うことにより、前記装置に
15 関する第1の情報、及び、前記第2の手段によって受信された画像信号を復号化するために用いられる第2の情報を前記装置に入力するステップ(a)と、
ステップ(a)において入力された第1及び第2の情報を前記不揮発性メモリに書き込むステップ(b)と、
20 を具備する方法。
29. ステップ(a)とステップ(b)との間において、第2の情報を暗号化するステップをさらに具備する請求項28記載の方法。
30. 前記第1の手段を用いてシリアル通信を行うことにより、ステップ(b)において前記不揮発性メモリに書き込んだ情報を確認するステップ
25 をさらに具備する請求項28記載の方法。
31. 外部とシリアル通信を行う第1の手段と、暗号化された画像信号

を受信する第2の手段と、不揮発性メモリとを有し、暗号化された画像信号を受信する装置を修理する方法であって、

前記第1の手段を用いてシリアル通信を行うことにより、前記装置に関する第1の情報、及び、前記第2の手段によって受信された画像信号
5 を復号化するために用いられる第2の情報を前記装置に入力するステップ(a)と、

ステップ(a)において入力された第1及び第2の情報をを用いて、前記不揮発性メモリに記憶されている情報を書き替えるステップ(b)と、

10 を具備する方法。

32. ステップ(a)とステップ(b)との間において、第2の情報を暗号化するステップをさらに具備する請求項31記載の方法。

33. 暗号鍵を入力する第1の手段と、暗号化された画像信号を受信する第2の手段とを有し、暗号化された画像信号を受信して画像を表示する受像機を用いて画像を提供する方法であって、
15

前記第1の手段によって受像機に入力された暗号鍵に基づいて、前記受像機を認証するか否かについて判断するステップ(a)と、

ステップ(a)において前記受像機が認証された場合に、前記第2の手段によって受信された画像信号を前記第1の手段によって受像機に入力された暗号鍵を用いて復号化し、復号化された画像信号に基づいて画像を表示するステップ(b)と、
20 を具備する方法。

1/9

FIG.1

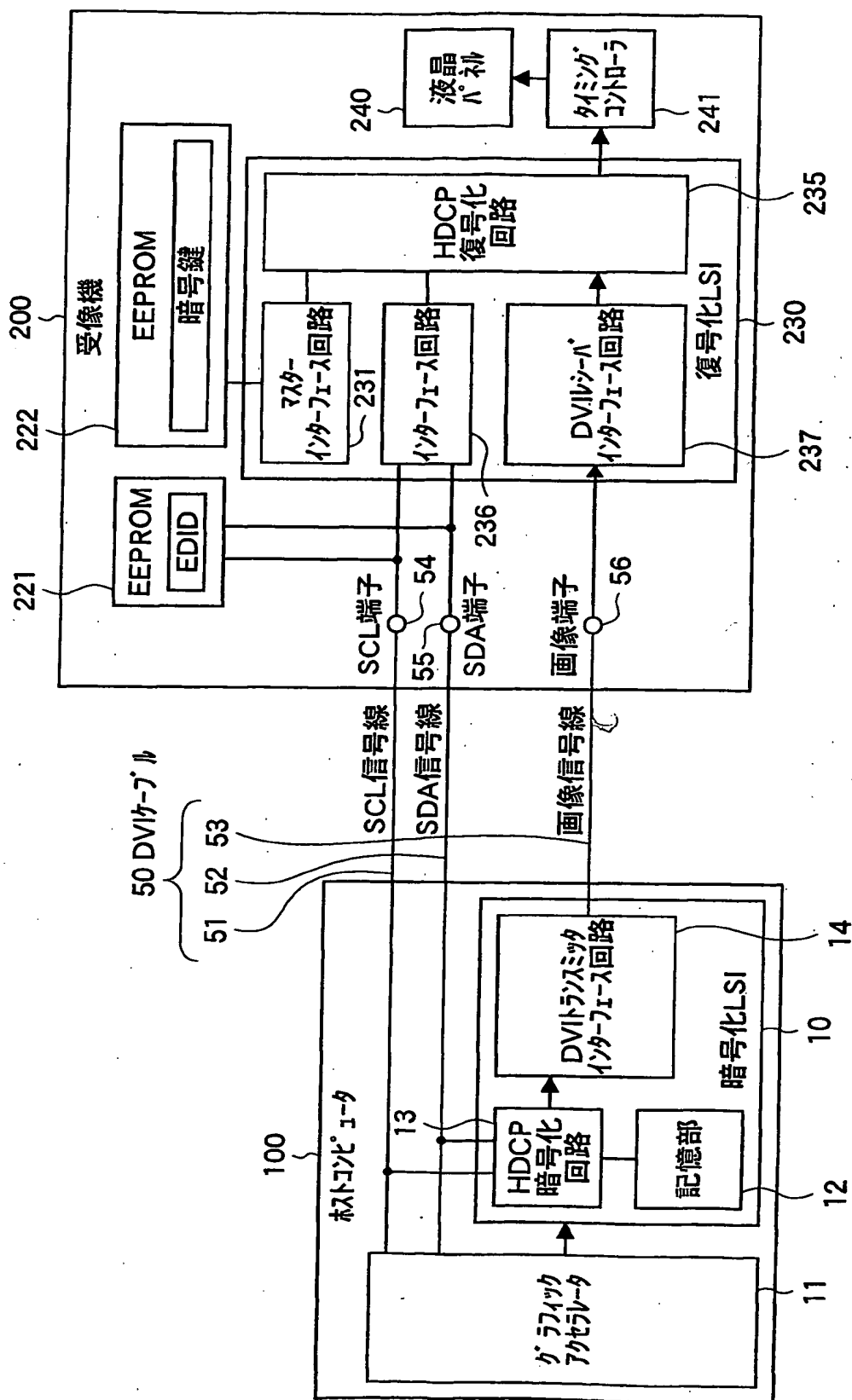


FIG.2

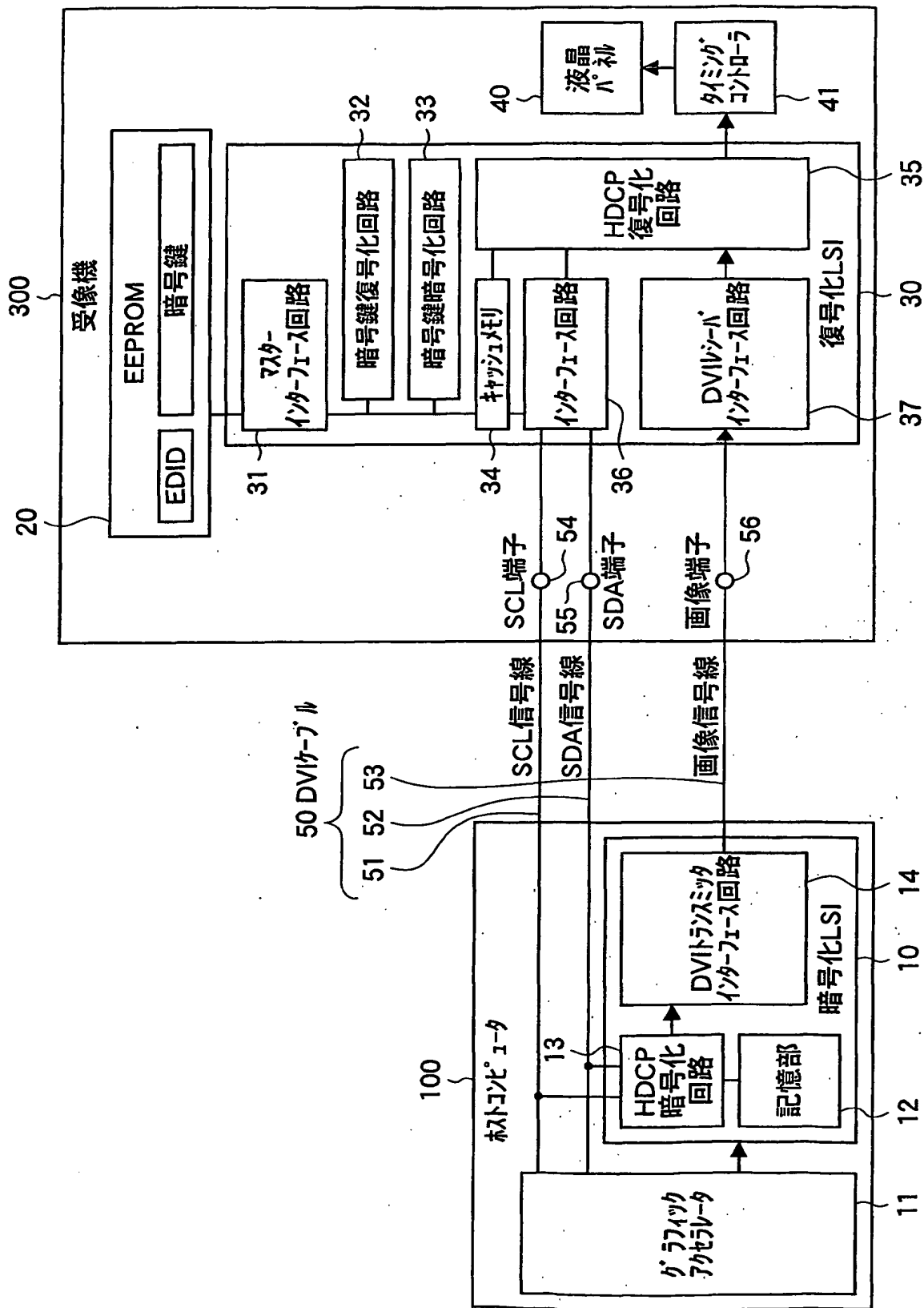
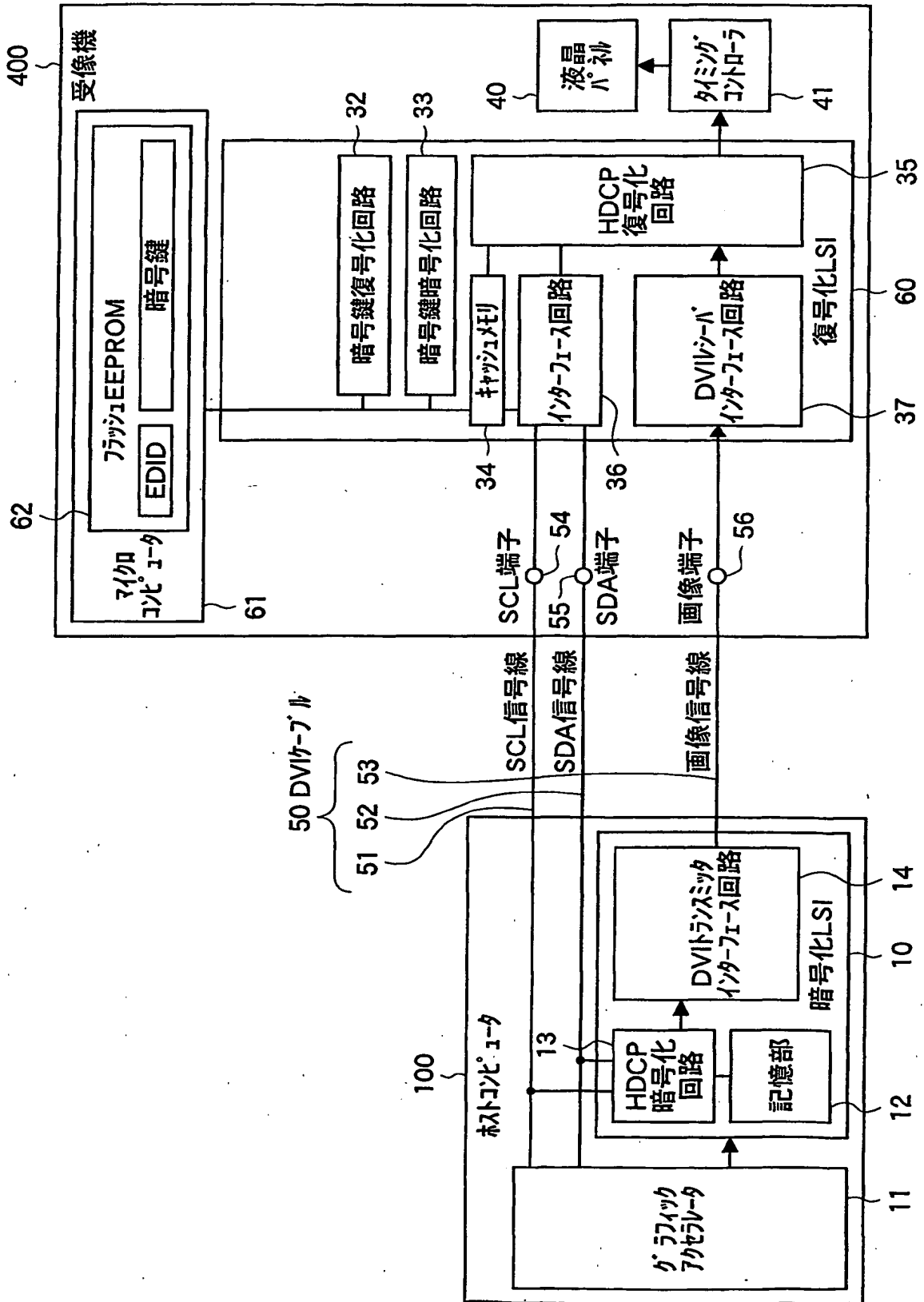
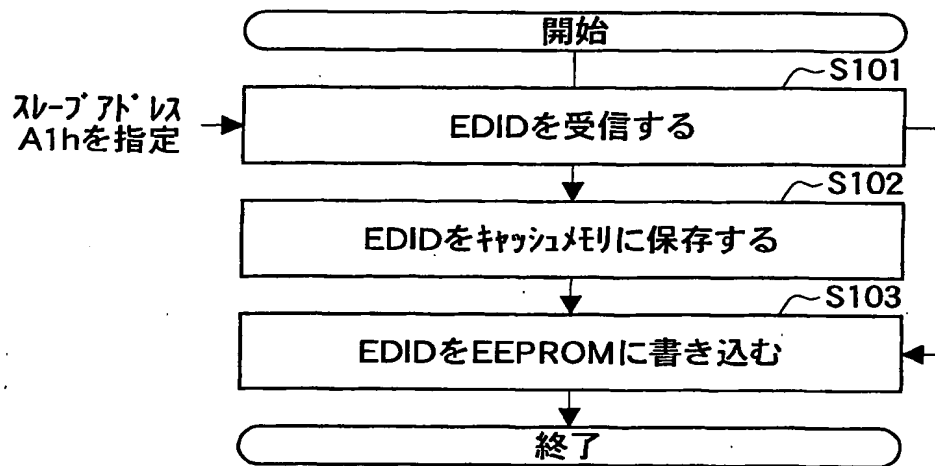
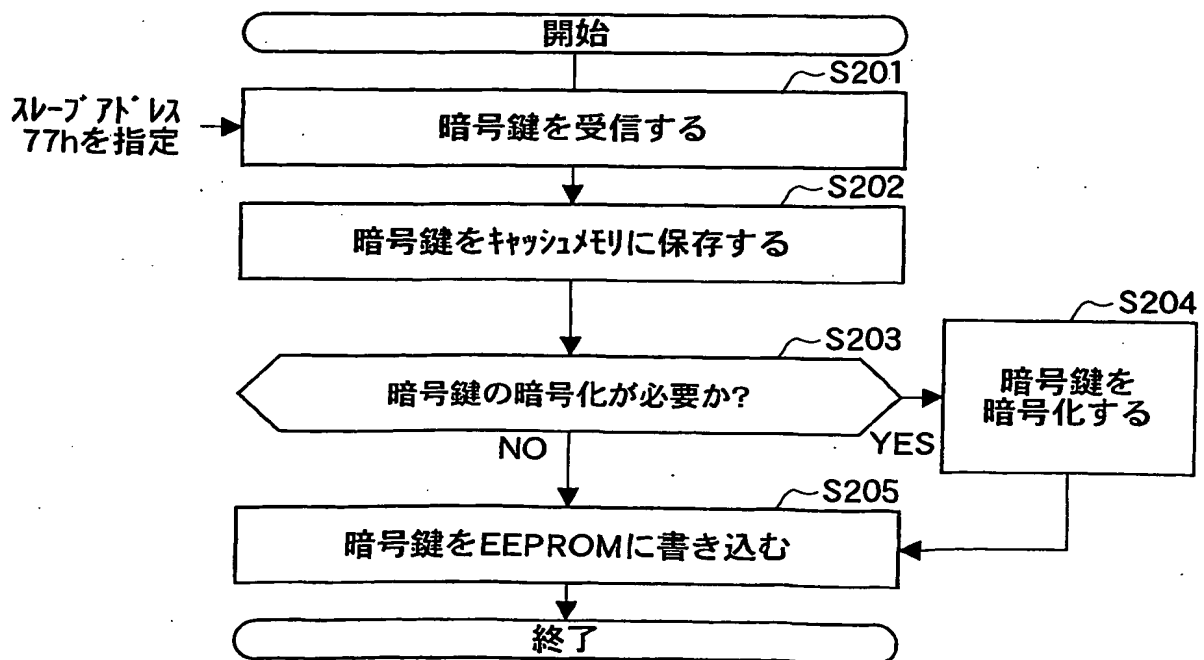


FIG.3

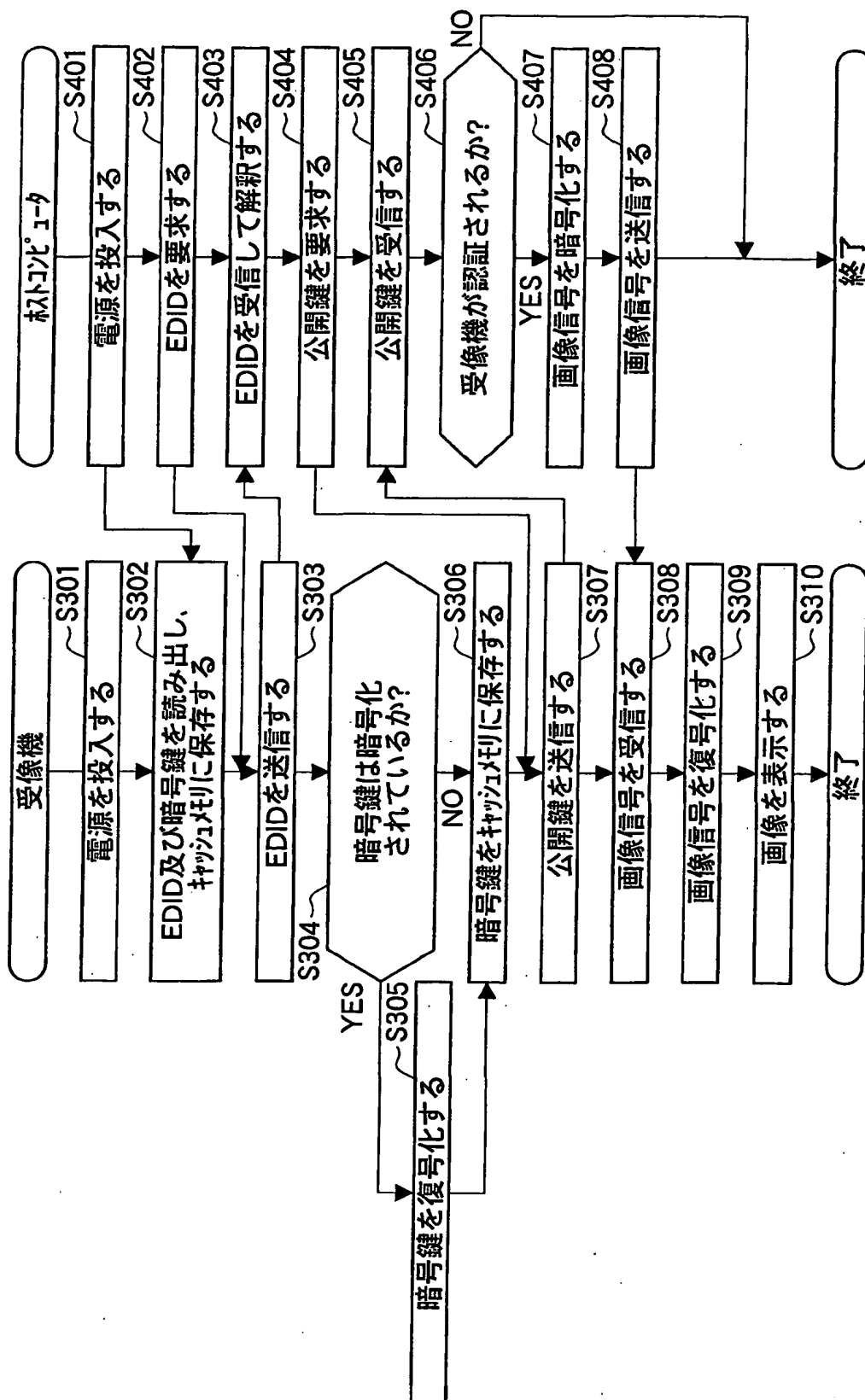


4/9

FIG.4**FIG.5**

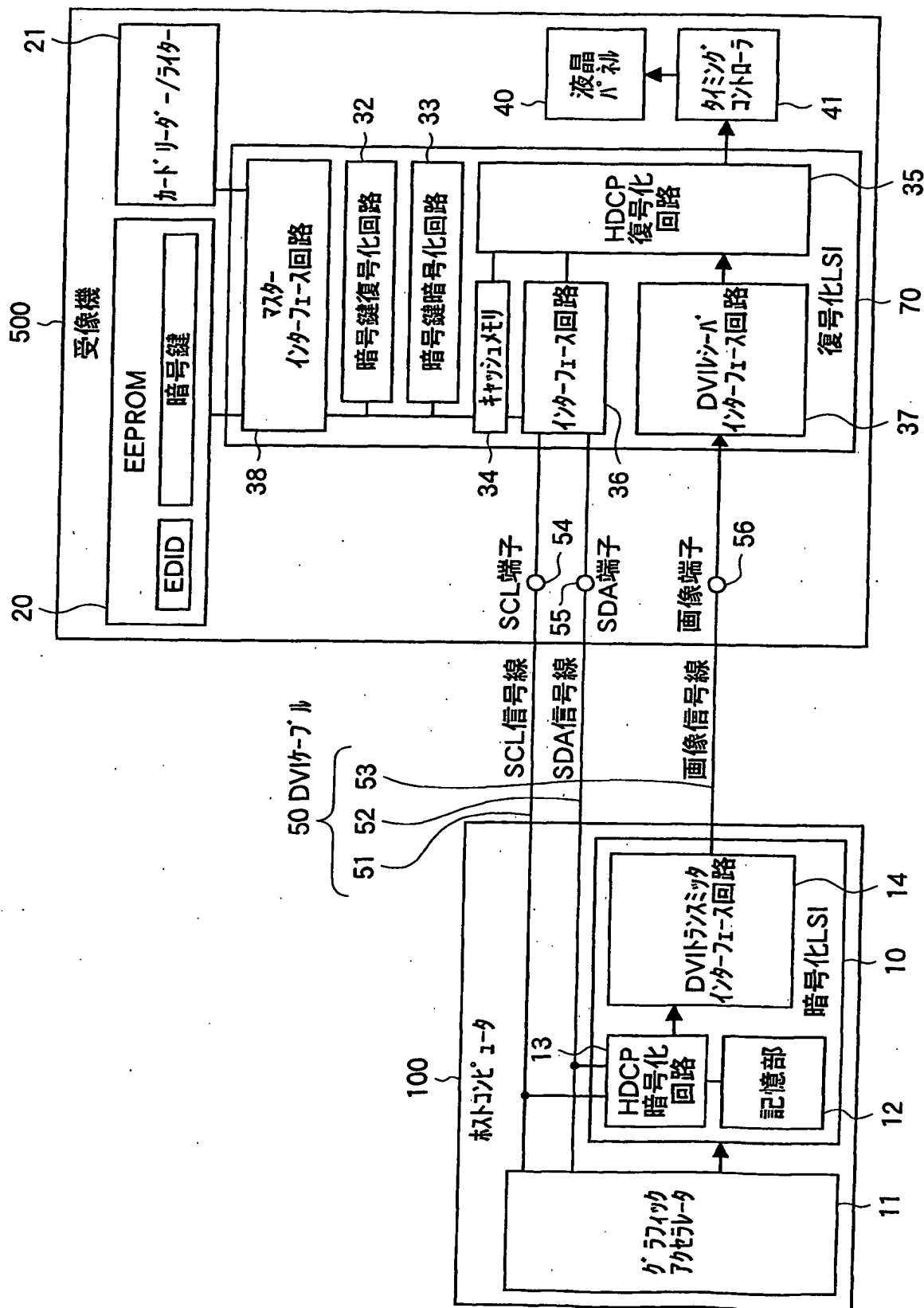
5/9

FIG.6



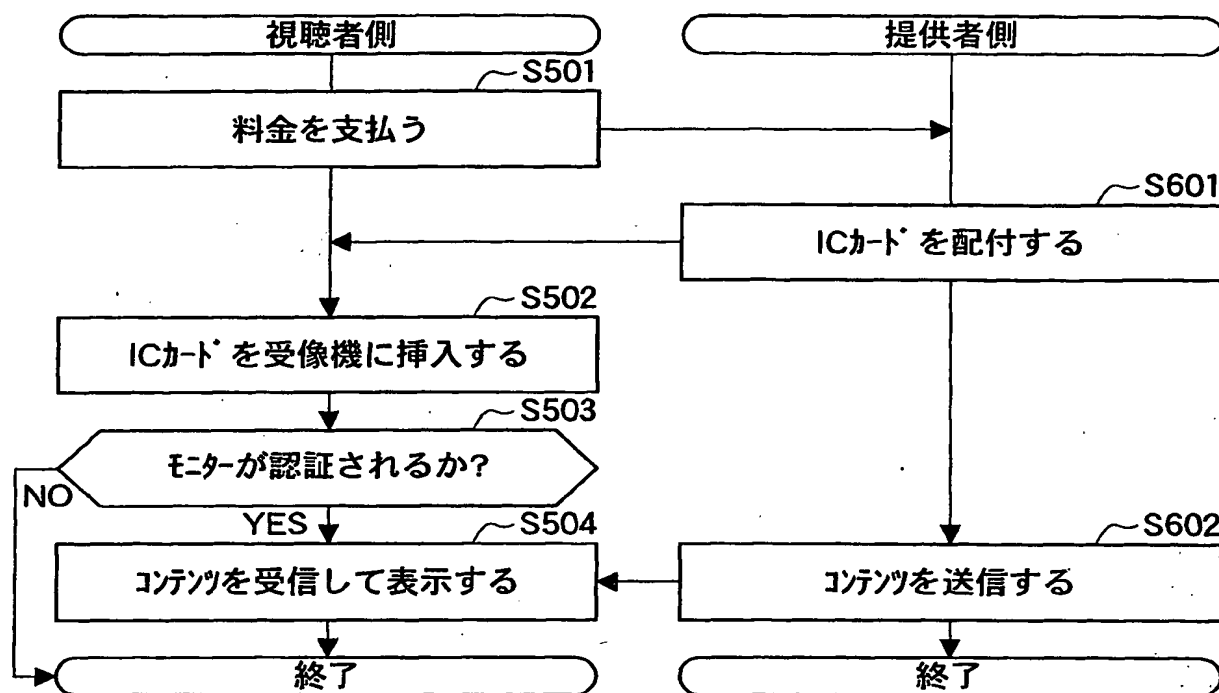
6/9

FIG.7



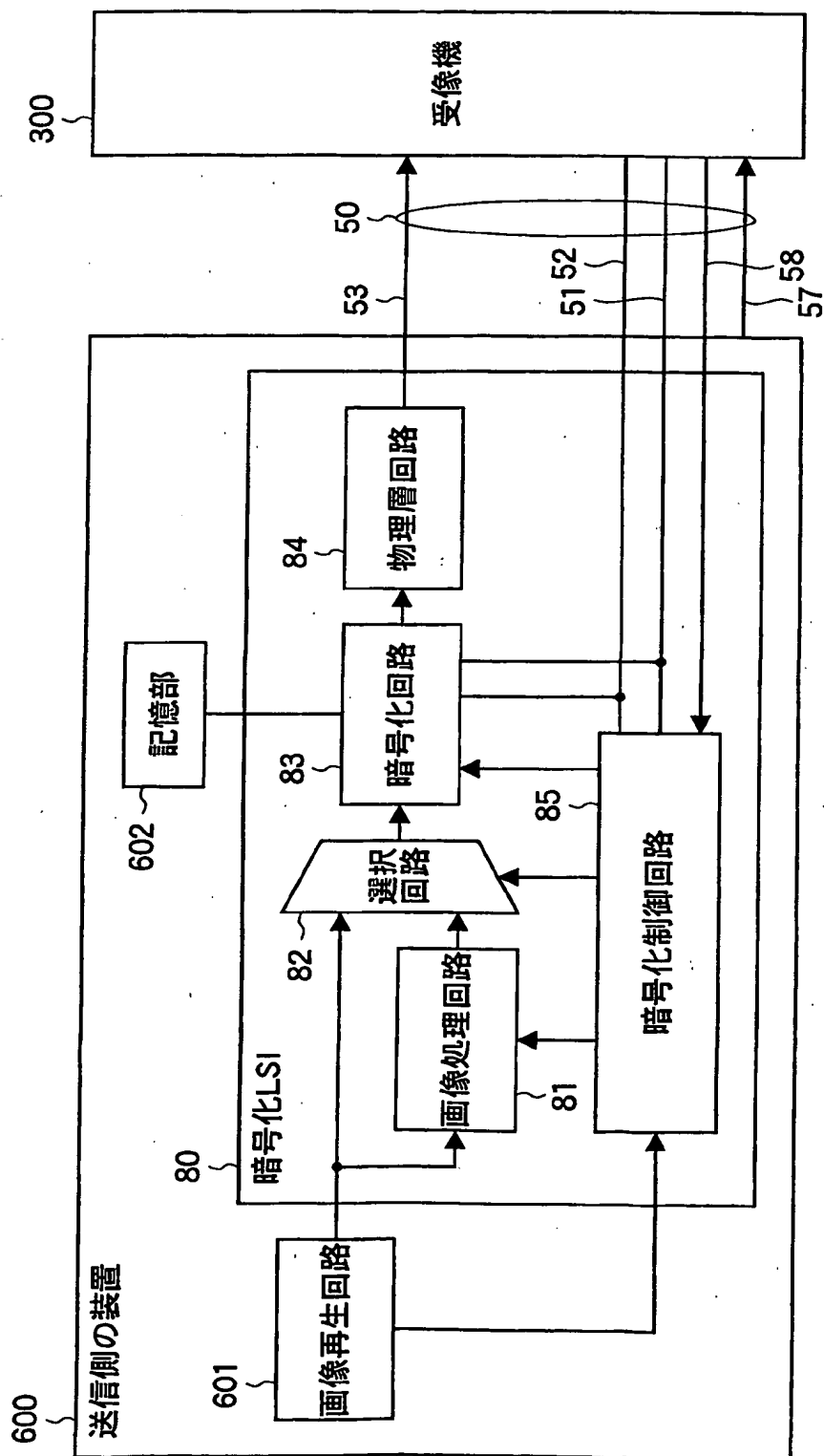
7/9

FIG.8



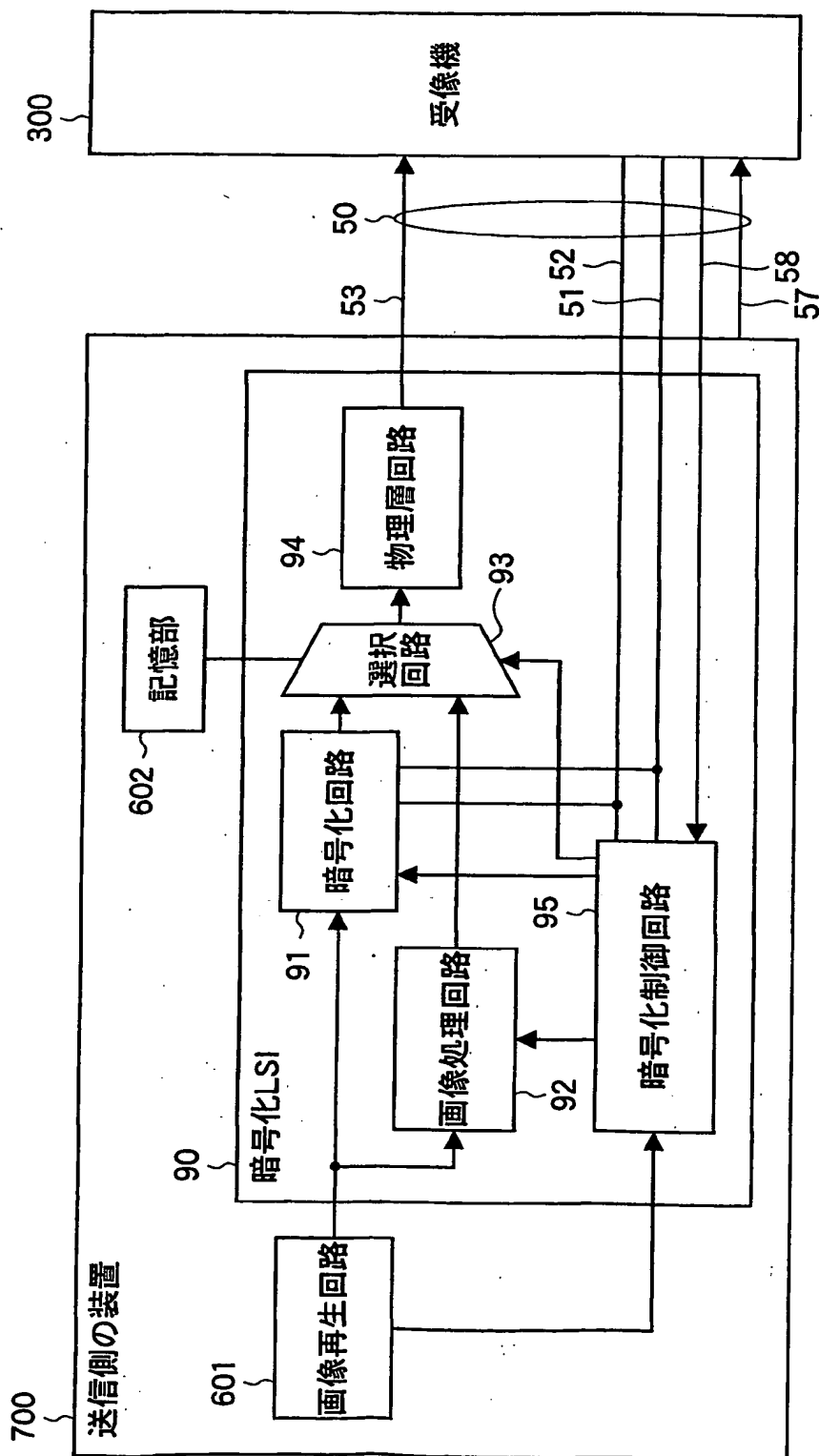
8/9

FIG.9



9/9

FIG.10



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/09279

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F12/14, G09G 5/00, H04N 7/16,
H04N 1/00, H04N 1/44

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F12/14, G09G 5/00, H04N 7/16,
H04N 1/00, H04N 1/44

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Toroku Jitsuyo Shinan Koho	1994-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	High-bandwidth Digital Content Protection. WHITE PAPER. [online]. Silicon Image, Inc. February 2000. [retrieved on 2002-01-11]. Retrieved from the Internet: <URL: http://www.siimage.com/documents/ SiI-WP-002-A.pdf>.	1-33
Y	JP 11-73375 A (Dainippon Printing Co., Ltd.), 16 March, 1999 (16.03.1999), Full text; Figs. 1 to 5 (Family: none)	1-33
Y	JP 2000-181802 A (Matsushita Electric Ind. Co., Ltd.), 30 June, 2000 (30.06.2000), Full text; Figs. 1 to 5 (Family: none)	1-33
Y	JP 8-185361 A (Hitachi, Ltd.), 16 July, 1996 (16.07.1996), Full text; Figs. 1 to 4 (Family: none)	1-33
Y	WO 99/07150 A (SCIENTIFIC-ATLANTA, INC.), 11 February, 1999 (11.02.1999), Full text; Figs. 1 to 29 & JP 2001-512842 A	1-33

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
 "A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier document but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 "&" document member of the same patent family

Date of the actual completion of the international search
15 January, 2002 (15.01.02)

Date of mailing of the international search report
29 January, 2002 (29.01.02)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/09279

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-194603 A (Dainippon Printing Co., Ltd.), 14 July, 2000 (14.07.2000), Full text; Figs. 1 to 7 (Family: none)	4-7, 19, 20
Y	JP 8-6879 A (Toshiba Corporation), 12 January, 1996 (12.01.1996), Full text; Figs. 1 to 4 (Family: none)	14, 15, 33
Y	JP 6-197104 A (Sony Corporation), 15 July, 1994 (15.07.1994), Full text; Figs. 1 to 5 (Family: none)	26
Y	JP 9-97216 A (Sony Corporation), 08 April, 1997 (08.04.1997), Full text; Fig. 16 (Family: none)	27
Y	JP 2000-194346 A (NEC Home Electronics Ltd.), 14 July, 2000 (14.07.2000), Full text; Figs. 1 to 3 (Family: none)	28-32

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, G09G 5/00, H04N 7/16,
H04N 1/00, H04N 1/44

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, G09G 5/00, H04N 7/16,
H04N 1/00, H04N 1/44

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922 - 1996年
日本国公開実用新案公報 1971 - 2002年
日本国実用新案登録公報 1996 - 2002年
日本国登録実用新案公報 1994 - 2002年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	High-bandwidth Digital Content Protection. WHITE PAPER. [online]. Silicon Image, Inc. February 2000. [retrieved on 2002-01-11]. Retrieved from the Internet: <URL: http://www.siimage.com/documents/SiI-WP-002-A.pdf >.	1-33
Y	J P 11-73375 A (大日本印刷株式会社) 1999. 03. 16, 全文, 第1-5図 (ファミリーなし)	1-33

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

15. 01. 02

国際調査報告の発送日

29.01.02

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号 100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

相崎 裕恒

5 N 3044

電話番号 03-3581-1101 内線 3585

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2000-181802 A (松下電器産業株式会社) 2000. 06. 30, 全文, 第1-5図 (ファミリーなし)	1-33
Y	JP 8-185361 A (株式会社日立製作所) 1996. 07. 16, 全文, 第1-4図 (ファミリーなし)	1-33
Y	WO 99/07150 A (SCIENTIFIC-ATLANTA, INC.) 1999. 02. 11, 全文, 第1-29図 & JP 2001-512842 A	1-33
Y	JP 2000-194603 A (大日本印刷株式会社) 2000. 07. 14, 全文, 第1-7図 (ファミリーなし)	4-7, 19, 20
Y	JP 8-6879 A (株式会社東芝) 1996. 01. 12, 全文, 第1-4図 (ファミリーなし)	14, 15, 33
Y	JP 6-197104 A (ソニー株式会社) 1994. 07. 15, 全文, 第1-5図 (ファミリーなし)	26
Y	JP 9-97216 A (ソニー株式会社) 1997. 04. 08, 全文, 第16図 (ファミリーなし)	27
Y	JP 2000-194346 A (日本電気ホームエレクトロニクス株式会社) 2000. 07. 14, 全文, 第1-3図 (ファミリーなし)	28-32